Lecture 1

Some problems in number theory.

I. Counting integral solutions.

Consider a system of polynomial equations:

$$X = \{ f_1(x_1, \dots x_d) = \dots = f_N(x_1, \dots x_d) = 0 \};$$

$$f_1, \dots f_N \in \mathbb{Z}[x_1, \dots x_d]$$

Let $N_T(X) = \#\{ x \in \mathbb{Z}^d \cap X : \max |x_i| \le T \}$.

Conj (Chambert-Loir, Tschinkel)
For a "general class" of X,

$$N_T(X) \sim c \cdot T^a (\log T)^b \text{ as } T \to \infty,$$

for $c > 0$, $a \in \mathbb{Q}^+$, $b \in \mathbb{N}_0$.
(a, b are determined explicitly by geometry of $X/\mathbb{C}$)

II. Oppenheim Conj (1929)

$$Q(x_1, \dots x_d) = \sum_{i,j=1}^{d} a_{ij} x_i x_j, \quad a_{ij} \in \mathbb{R}$$

Assume that:
- $d \ge 3$,
- Q is nondegenerate ($\det(a_{ij}) \neq 0$),
- Q is indefinite ($Q(\mathbb{R}^d) = \mathbb{R}$).
- Q is irrational ($Q \neq \alpha \cdot Q_0$, where Q_0 has rational coefficients).

Then $Q(\mathbb{Z}^d)$ is dense in $\mathbb{R}$.

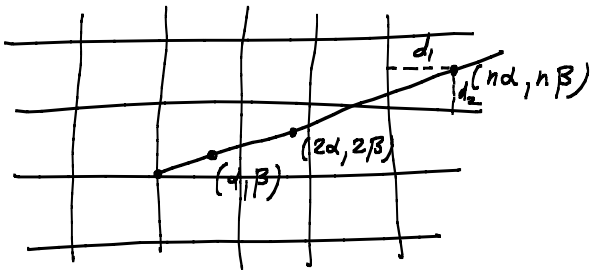
Proved by Margulis in 1987.

Ex. $\{x^2+y^2-\sqrt{2}z^2 : x,y,z \in \mathbb{Z}\}$ is dense in $\mathbb{R}$.

III. Littlewood Conj ('1930)

For every $\alpha, \beta \in \mathbb{R}$,

$$\liminf_{n\to\infty} n \cdot d(n\alpha, \mathbb{Z}) \cdot d(n\beta, \mathbb{Z}) = 0$$



$n \cdot d_1(n) \cdot d_2(n) \approx 0.$

Still Open !

IV. Diophantine approximation

Given $x \in \mathbb{R}^d$, how well can we approximate x by rational vectors: $x \approx \frac{p}{q}$.

Fix $\psi : \mathbb{R}^+ \longrightarrow \mathbb{R}^+$.

The vector x is called ψ-approximable if

$$\|x - \tfrac{p}{q}\| \leq \frac{\psi(q)}{q}$$

has infinitely many solutions.

Thm (Khinchin – Groshev)

"Typical" $x \in \mathbb{R}^d$ are ψ-approximable

$$\Updownarrow$$

$$\sum_{\ell \geq 1} \psi(\ell)^d = \infty$$

ex. For "typical" x,

$\|x - \frac{p}{q}\| \leq q^{-1-\frac{1}{d}}$ has inf. many solutions,

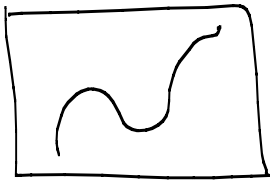
but $\|x - \frac{p}{q}\| \leq q^{-1-\frac{1}{d}-\varepsilon}$, $\varepsilon > 0$, only finitely many.

Def. 1) $x \in \mathbb{R}^d$ is *badly approximable* if
$\exists c > 0 : \forall p \in \mathbb{Z}^d \; \forall q \in \mathbb{N} \quad \|x - \frac{p}{q}\| > \frac{c}{q^{1+\frac{1}{d}}}$.

2) $x \in \mathbb{R}^d$ is *well approximable* if for some $\varepsilon > 0$,
$$\|x - \frac{p}{q}\| \leq \frac{1}{q^{1+\frac{1}{d}+\varepsilon}}$$
has infinitely many solutions.

⟶ The set of badly approximable vectors is a complicated fractal set

⟶ "Typical" vectors in $\mathbb{R}^d$ are not well approximable.



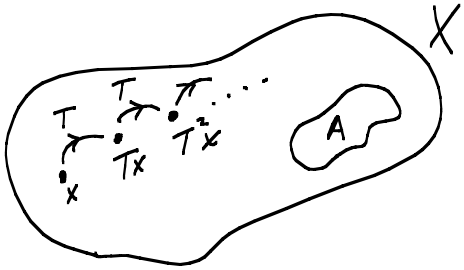
Conj (Sprindzuk; 1980)
If X is a "curved" surface in $\mathbb{R}^d$ then "typical" $x \in X$ is not well approximable.

Proved by Kleinbock – Margulis in 1998.

Introduction to dynamical systems.

A dynamical system consists of a space X, and a transformation

$$T : X \longrightarrow X$$



Orbit: $\{x, Tx, T^2x, \ldots\}$

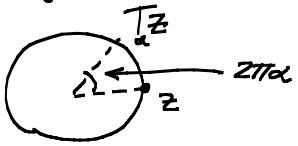
Basic problem: Understand distribution of orbits:

given $A \subset X$, $\dfrac{\#\{i=0,\dots N : T^i x \in A\}}{N+1} \xrightarrow[N\to\infty]{}$?

Two Examples:

$X = S^1 = \{z \in \mathbb{C} : |z| = 1\}$.

1) rotation: $T_\alpha : S^1 \to S^1 : z \mapsto e^{2\pi i \alpha} z$



2) doubling: $D_2 : S^1 \to S^1 : z \to z^2$.

Def. T is called *mixing* if $\forall \varphi_1, \varphi_2 : X \to \mathbb{C}$

$$\int_X \varphi_1(T^n x)\varphi_2(x)\,dx \xrightarrow[n\to\infty]{} \left(\int_X \varphi_1\right)\cdot\left(\int_X \varphi_2\right).$$

(compare with notion of *independence* in Probability: observables $\varphi_1 \circ T^n$ and φ_2 become asymptotically independent).

Prop. The doubling map $D_2 : S^1 \to S^1$ is mixing.

Fourier analisys:

first, consider $\varphi_1(z) = z^{n_1}$, $\varphi_2(z) = z^{n_2}$ - characters.

Recall that $\int_{S^1} z^n dz = \begin{cases} 0, & n \neq 0, \\ 1, & n = 0. \end{cases}$

$$\int_{S^1} \varphi_1(D_2^n z)\varphi_2(z)\,dz = \int_{S^1} z^{2^n n_1 + n_2}\,dz = \begin{cases} 1, & n_1 = n_2 = 0, \\ 0, & n_1 \neq 0 \text{ or } n_2 \neq 0 \\ & \text{and } n \gg 0. \end{cases}$$

Hence, $\int_{S'} (\varphi_1 \circ D_2^n)\varphi_2 \, dz = \left(\int_{S'} \varphi_1\right)\left(\int_{S'} \varphi_2\right)$ for sufficiently large n.

Next, any continuous function on S' can be approximated by linear combinations of characters....

Prop. Let $\alpha \in \mathbb{R} \setminus \mathbb{Q}$. Then for every $x \in S'$, interval $A \subset S'$

$$\frac{\#\{i = 0, \dots N : T_\alpha x \in A\}}{N+1} \xrightarrow[N\to\infty]{} |A|.$$

(in particular, every orbit is dense.)

We need to show that $\frac{1}{N+1}\sum_{n=0}^{N} \chi_A(T_\alpha^n x) \to \int_{S'} \chi_A$, where χ_A is the characteristic function of A.

Approximate χ_A by linear combinations of characters...

Then we need to show that

$$\frac{1}{N+1}\sum_{n=0}^{N} \varphi(T_\alpha^n x) \to \int_{S'} \varphi$$

for $\varphi(z) = z^m$. For $m \neq 0$,

$$\frac{1}{N+1}\sum_{n=0}^{N} \left(e^{2\pi i n\alpha} x\right)^m = \frac{x^m}{N+1}\sum_{n=0}^{N} \left(e^{2\pi i m\alpha}\right)^n$$

$$= \frac{x^m}{N+1} \cdot \frac{\left(e^{2\pi i m\alpha}\right)^{N+1} - 1}{e^{2\pi i m\alpha} - 1} \xrightarrow[N\to\infty]{} 0,$$

since $e^{2\pi i m\alpha} \neq 1$.

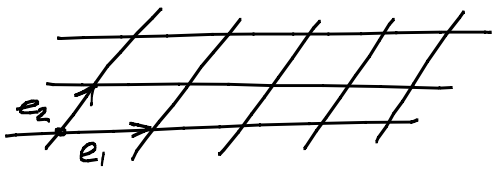
→ "Typical" orbits of the doubling map D_2 are dense in S', but there are many complicated orbits

Thm (Furstenberg) Let p, q $(p \neq q)$ be primes, and $z \in e^{2\pi i \mathbb{Q}}$. Then

$$\overline{\{D_p^m D_q^n z : m, n \geq 0\}} = S^1.$$

→ This property is related to the Littlewood Conj.

Space of lattices



a lattice in $\mathbb{R}^d$ is a subgroup $L = \mathbb{Z}v_1 + \dots + \mathbb{Z}v_d$ for a basis $\{v_i\}$ of $\mathbb{R}^d$.

Let $\mathcal{L}_d = \{$set of all lattices in $\mathbb{R}^d\}$.

$\mathcal{B}_d = \{$set of all basises$\} = \{(v_1, \dots v_d) : v_i \in \mathbb{R}^d, \det(v_1, \dots v_d) \neq 0\}$

$(v_1, \dots, v_d) \sim (v_1', \dots v_d')$ if

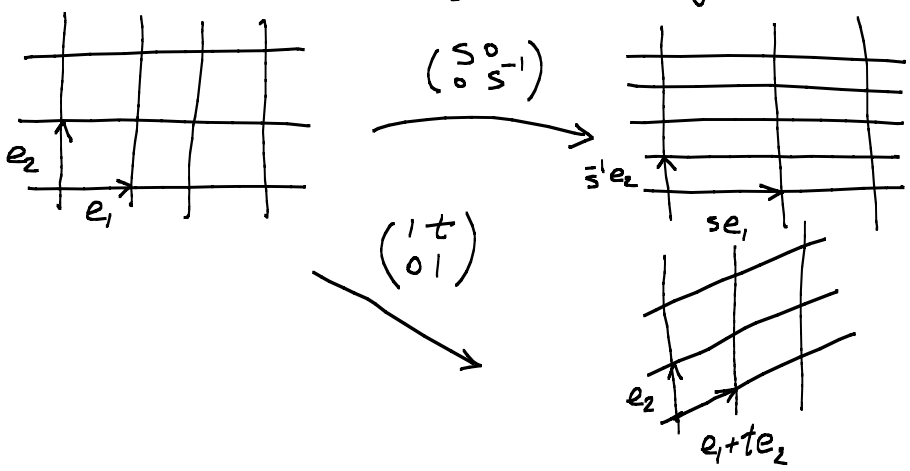
$\mathbb{Z}v_1 + \dots + \mathbb{Z}v_d = \mathbb{Z}v_1' + \dots + \mathbb{Z}v_d'$.

Then $\mathcal{L}_d \simeq \mathcal{B}_d / \sim$.

$G = GL_d(\mathbb{R}) = \{g \in Mat_d(\mathbb{R}) : \det(g) \neq 0\}$.

The group G acts on $\mathcal{B}_d$ and $\mathcal{L}_d$:

$$\{v_i\} \xrightarrow{g} \{v_i g\}$$



Note that G acts transitively on $\mathcal{B}_d$ and $\mathcal{L}_d$.

Let $\{e_i\}$ be the standard basis.

If $g \cdot \{e_i\} = \{e_i\}$, then $g = id$, so that

$$\mathcal{B}_d \simeq GL_d(\mathbb{R}).$$

If $g(\mathbb{Z}e_1 + \dots + \mathbb{Z}e_d) = \mathbb{Z}e_1 + \dots + \mathbb{Z}e_d$, then

$g \in Mat_d(\mathbb{Z})$ and $g^{-1} \in Mat_d(\mathbb{Z})$,

equivalently, $g \in Mat_d(\mathbb{Z})$ and $\det(g) = \pm 1$.

Converse also holds.

Hence, $Stab_G(\mathbb{Z}e_1 + \dots + \mathbb{Z}e_d) = \underbrace{\{g \in Mat_d(\mathbb{Z}) : \det(g) = \pm 1\}}_{GL_d(\mathbb{Z})}$,

and $\boxed{\mathcal{L}_d \simeq GL_d(\mathbb{Z}) \backslash GL_d(\mathbb{R}).}$

The space $\mathcal{L}_d$ is equiped with natural topology and (finite, invariant) measure.

Measure

A measure μ on X is a map $\mu : \{\text{subsets of } X\} \to \mathbb{R}^+ \cup \{\infty\}$ such that:

1) $\mu(\emptyset) = 0$

2) $\mu\left(\bigcup_{i \geq 1} A_i\right) = \sum_{i \geq 1} \mu(A_i)$ for every $A_i \subset X$ such that $A_i \cap A_j = \emptyset$ for $i \neq j$.

In general, it is impossible to define μ on all subsets of X consistently, but only on a "large"

family of subsets (called measurable subsets).

Alternatively, one can think of μ as

$$\mu : \{\text{functions on } X\} \longrightarrow \mathbb{C}.$$

ex. Lebesgue measure $\lambda : \{\text{measurable subsets of } \mathbb{R}^d\} \to \mathbb{R}^+ \cup \{\infty\}$,

$$\lambda\left(\prod_{i=1}^{d}(a_i, b_i)\right) = \prod_{i=1}^{d}(b_i - a_i).$$

Invariant measure on $GL_d(\mathbb{R})$ (Haar measure)

Thm $G = GL_d(\mathbb{R})$. The measure μ defined by

$$\int_G f(g) \cdot \frac{\left(\prod_{i,j=1}^{d} dg_{ij}\right)}{\det(g)^d}$$

is invariant under left/right multiplication.

(That is, $\int_G f(g_0 g)\, d\mu(g) = \int_G f(g)\, d\mu(g)$.)

For $g_0 \in G$, the map $h \longmapsto g_0 h = g$ defines a differential transformation of $Mat_d(\mathbb{R})$ with $Jac(h \longmapsto g_0 h) = \det(g_0)^d$. Hence,

$$\int_G f(g) \cdot \frac{\left(\prod_{i,j} dg_{ij}\right)}{\det(g)^d} = \int_G f(g_0 h) \cdot Jac(h \to g_0 h) \cdot \frac{\left(\prod_{i,j} dh_{ij}\right)}{\det(g_0 h)^d}$$

$$= \int_G f(g_0 h) \frac{\left(\prod_{i,j} dh_{ij}\right)}{\det(h)^d}.$$

$\longrightarrow$ Invariant measures exist on every loc. compact group. Moreover, such measure is unique up to a scalar multiple.